Annales Univ. Sci. Budapest., Sect. Comp. 28 (2008) 157-174

ON REPRESENTING INTEGERS AS QUOTIENTS OF SHIFTED PRIMES

T. Csajbók, A. Járai and J. Kasza

(Budapest, Hungary)

Dedicated to Prof. Imre Kátai
on the occasion of his 70th birthday

Abstract. For all integers $2 \leq Q \leq 10^{11}$ we have found the representation of the form $\frac{p+1}{q+1}$, where p and q are the smallest possible primes. We have also done the same for all primes Q over a larger interval $2 \leq Q \leq 10^{14}$. The results are tabulated and the methods are explained.

A function $f : \mathbb{N} \to \mathbb{R}$ is said to be completely additive, if $f(mn) = f(m) + f(n)$ holds for every pair of integers m and n. Let $\mathcal{A}^*$ be the class of completely additive functions. Let $\mathcal{P}$ be the set of primes, a general element of which is denoted by p with or without subscripts.

Let $\mathcal{P}_a = \{p + a \mid p \in \mathcal{P}\}$ the set of shifted primes. Here $a \neq 0$ is a fixed integer. I. Kátai [1] introduced the following notions.

Let $E \subseteq \mathbb{N}$. We say that E is a set of uniqueness (with respect to $\mathcal{A}^*$), if $f \in \mathcal{A}^*$ and $f(E) = 0$ imply that $f(\mathbb{N}) = 0$. (Here $f(E) = \{f(n) \mid n \in E\}$ if $E \subset \mathbb{N}$.)

Furthermore he posed the question whether the set $\mathcal{P}_1$ is a set of uniqueness or not. In [2] he proved that there exists a finite set of primes $\{q_1, \ldots, q_k\}$ such that $\{q_1, \ldots, q_k\} \cup \mathcal{P}_1$ is a set of uniqueness.

The above conjecture of Kátai has been proved by P.D.T.A. Elliot [3]. D. Wolke [4] and independently Dress and Volkman [5] proved that E ($\subset \mathbb{N}$) is a

set of uniqueness if and only if every $n \in \mathbb{N}$ can be written as $n = e_1^{r_1} \dots e_k^{r_k}$, where $e_1, \dots, e_k \in E$, $r_1, \dots, r_k \in \mathbb{Q}$.

We say that E ($\subset \mathbb{N}$) is a "set of uniqueness mod 1" if $f \in \mathcal{A}^*$ and $f(E) \subset \mathbb{Z}$ imply that $f(\mathbb{N}) \subset \mathbb{Z}$. Meyer [6], Indlekofer [7], Dress and Volkman [5], Hoffman [8] (see also Elliot [9]) proved that in order for E to be a set of uniqueness mod 1 it is necessary and sufficient that everz positive integer n has a representation

$$n = \prod_{j=1}^{s} e_j^{d_j}$$

with some integers (positive, negative or 0) d_j.

Probably, the set of $\mathcal{P}_1$ is a set of uniqueness mod 1. In the paper [2] I. Kátai proved implicitly that there is a constant L such that every integer n has a representation

$$n = A \cdot \prod_{i=1}^{k} (p_i + 1)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1,$$

where A is a rational number in the reduced form of which all prime factors of its numerator and denominator are less than L. The constant L was implicit, since he used the Bombieri-Vinogradov theorem.

Later Elliot [9] proved that $L = 10^{387}$ is appropriate. This means that it is sufficient to check that all primes $Q < L$ can be represented in the form $\frac{p+1}{q+1}$, where $p, q \in \mathcal{P}$. This bound is extremely large for computational purposes. We remark that in 1958 Schinkel and Sierpinski [8] posed the conjecture that every positive integer number has infinitely many representations of form $\frac{p+1}{q+1}$ with $p, q \in \mathcal{P}$.

Our plan was to check the existence of such representations for primes Q as high as possible by using computers. The limit we have reached is far below 10^{387}, but the improvement of the theoretical upper bound is expected. We also checked whether composite Q's can be represented in this form, but we used only limited resources for these checks because the faster of two primality tests we applied to test p does not work in this general case. To find the smallest possible representation as quotient of shifted primes for a fixed Q we try all primes q up until the value of $Q \cdot (q + 1) - 1$ becomes prime. Our main goal was to create a table of the first occurences of the largest q values. To this end we developed a program in C and Assembly and highly optimized it for the AMD64 architecture.

The most important methods in our research were to find an efficient way to produce and test primes. The trying of q's equals producing a table of prime numbers, which we did by using the well-known sieve of Eratosthenes. Then, for each q we tested the primality of $Q \cdot (q+1) - 1$. Obviously, we could not base

our prime tests on any kind of probability tests. Only the provable primality tests are accepted and that is a significant restriction of our possibilities.

For $Q < 10^{11}$ we used the deterministic variant of the Miller-Rabin primality test with some improvements. Normally, this test proves only compositeness. For a prime number it tells only that the number is prime with a high probability - because strong pseudo-primes can also pass the test. The list of base-2 pseudo-primes is known up to 341,550,071,728,321. Using this list, we can compute strong pseudo-primes to any set of bases containing 2. For example up to $25 \cdot 10^9$ there are 13 strong pseudo-primes to bases 2, 3 and 5, see the paper of Pomerance, Selfridge and Wagstaff [12]. Furthermore, the first pseudo-primes to bases 2, 3, 5, 7 and 11 is 2,152,302,898,747, to bases 2, 3, 5, 7, 11 and 13 is 3,474,749,660,383 and to bases 2, 3, 5, 7, 11, 13 and 17 is 341,550,071728,321, see Jaeschke [13].

With these improvements we have a primality test for p up to around 10^{14}, but not above. We gained further speed up by computing the greatest common divisor of p and the product of all small primes that fit into one 64-bit machine word so as to quickly determine small divisors.

To reach the upper limit 10^{14} for primes Q the form $p = Q \cdot (q+1) - 1$ suggests using a Lucas-type prime test, which works as follows:

Let $n > 1$ be an odd integer, f a positive divisor of $n+1$ such that $\gcd(f, \frac{n+1}{f}) = 1$ and let D be the discriminant of the equation $\lambda^2 - P\lambda + 1 = 0$. Suppose that $\gcd(D, n) = 1$ and $(D|N) = -1$, where $(x|y)$ denotes the Jacobian symbol of x and y. Consider the Lucas sequence corresponding to this characteristic equation. If

$$V_{n+1} \equiv 2, \qquad U_{n+1} \equiv 0 \pmod{n},$$

and for each prime divisor m of f we have

$$\gcd(V_{(n+1)/m} - 2,\ U_{(n+1)/m},\ n) = 1,$$

then every divisor d of n satisfies $d \equiv \pm 1 \pmod{f}$ and if $f \geq \sqrt{n} + 2$ then n is prime.

In our case we set $n = Q \cdot (q+1) - 1$ and $f = Q$. This way we can use the above Lucas-type test because $\gcd(f, (n+1)/f) = \gcd(Q, q+1) = 1$.

This test can prove primality with a certain probability. To decide for a given $p = Q \cdot (q+1) - 1$ whether it is prime or composite we use the following procedure: First we compute the greatest common divisor of p and the product of small primes as mentioned above. Then we use the Miller-Rabin test to disprove primality and the above Lucas-type test to prove primality, one after the other, each time using a different base and a different P, respectively, until

we prove either primality or compositeness. However, this test works only if Q is a prime and $Q > q + 1$.

Our running environment has been a cluster in the Department of Computer Algebra, Faculty of Informatics, Eötvös Loránd University, Budapest. The processor type of all nodes has been AMD Athlon64 and the number of nodes we used varied between 16 and 36. When we reached the 10^{14} limit for Q we stopped the computing. Our total running time in CPU time was 7 years and 71 days.

We thank Prof. Imre Kátai very much for his suggestions and help on this paper.

Occurences of primes as q values for prime Q values (1)

prime	occurences of q	prime	occurences of q
2	1	103	13871399579
3	130012344950	107	48753016671
5	248259898481	109	17471895558
7	118925472004	113	42971191459
11	219133833112	127	9288217123
13	121079168663	131	40346890986
17	188561808207	137	37451666693
19	107755684665	139	12052492044
23	164672010085	149	42060116392
29	200009359722	151	6287914141
31	61101357997	157	5233528761
37	57920883145	163	5083468865
41	147571269023	167	31668489919
43	50410260597	173	23643202138
47	107741756062	179	30110075289
53	99127758153	181	4739863558
59	120796571373	191	19867667988
61	32262348280	193	2791365852
67	30514786318	197	20219523906
71	76121564119	199	3514139751
73	24677694980	211	2338701752
79	30563327694	223	2453317646
83	76793743262	227	16059467617
89	78905764714	229	2497237804
97	19277601669	233	15223926187
101	54388798858	239	17860372374

Occurences of primes as q values for prime Q values (2)

prime	occurences of q	prime	occurences of q
241	1446794993	467	2264290080
251	14282948182	479	2528976529
257	10584599436	487	42120708
263	10888156091	491	1647670219
269	12373690939	499	54099211
271	843377845	503	1853938602
277	760424848	509	2096031156
281	8283631291	521	1216424507
283	667245883	523	22793692
293	8761855593	541	25359873
307	767074526	547	23746967
311	7030293316	557	1281779242
313	447867716	563	1075185556
317	6508798596	569	1505449152
331	444912313	571	22098682
337	405454672	577	15299495
347	5794692961	587	1150942474
349	559518490	593	884670119
353	5092174450	599	1106833355
359	6729533210	601	14627541
367	236556078	607	9818960
373	268293702	613	9214823
379	326100338	617	756304204
383	4115071733	619	12118774
389	6131848930	631	8296235
397	148993786	641	634931202
401	3624095009	643	8163503
409	191736205	647	603745079
419	5439611145	653	541944987
421	119436538	659	832787424
431	2866653061	661	4679097
433	117435076	673	4229562
439	134300953	677	478232696
443	2558481532	683	438370904
449	3531645722	691	3773751
457	65158965	701	432384898
461	2882825251	709	4618327
463	55020480	719	524952919

Occurences of primes as q values for prime Q values (3)

prime	occurences of q	prime	occurences of q
727	3237892	991	156076
733	2020769	997	94803
739	3265842	1009	164227
743	325188373	1013	73415897
751	2033645	1019	103489200
757	1744137	1021	124485
761	320271054	1031	62378227
769	2899148	1033	86442
773	266819161	1039	106080
787	1168341	1049	96383333
797	365319709	1051	58342
809	353088592	1061	47750030
811	1262331	1063	63494
821	233360314	1069	61306
823	829449	1087	41116
827	231427154	1091	58198289
829	1003861	1093	35521
839	334346806	1097	43771280
853	676891	1103	40866754
857	208232027	1109	55366759
859	728287	1117	25678
863	152645754	1123	22917
877	404353	1129	33268
881	188581756	1151	29482205
883	392934	1153	17138
887	136104946	1163	32283417
907	289309	1171	18546
911	134496353	1181	25464859
919	424420	1187	32020810
929	166131983	1193	25001234
937	248475	1201	12584
941	105218085	1213	11672
947	106595441	1217	32077687
953	97053709	1223	22606850
967	158838	1229	29525925
971	80950076	1231	12758
977	84087736	1237	6897
983	80862788	1249	10712

Occurences of primes as q values for prime Q values (4)

prime	occurences of q	prime	occurences of q
1259	31993955	1543	295
1277	16926798	1549	492
1279	7835	1553	4370419
1283	15531840	1559	4811260
1289	22362537	1567	275
1291	4872	1571	2539224
1297	4690	1579	344
1301	15893902	1583	3042654
1303	3557	1597	188
1307	12066364	1601	2320134
1319	17426023	1607	2610233
1321	2746	1609	260
1327	2475	1613	2032659
1361	9050959	1619	3203084
1367	10853125	1621	129
1373	9319791	1627	96
1381	2273	1637	2666027
1399	3249	1657	66
1409	12833735	1663	88
1423	1599	1667	1902810
1427	9760418	1669	103
1429	2379	1693	91
1433	6189353	1697	1502087
1439	9297116	1699	74
1447	852	1709	2336809
1451	6703464	1721	1626122
1453	867	1723	33
1459	1118	1733	1289619
1471	771	1741	31
1481	5655202	1747	41
1483	849	1753	31
1487	5139594	1759	59
1489	744	1777	31
1493	4881237	1783	31
1499	6343194	1787	1203591
1511	4599478	1789	37
1523	3580947	1801	26
1531	333	1811	1021316

Occurences of primes as q values for prime Q values (5)

prime	occurences of q	prime	occurences of q
1823	976390	2113	1
1831	23	2129	259228
1847	1295137	2141	189578
1861	19	2143	1
1867	14	2153	138465
1871	981499	2179	2
1873	10	2203	1
1877	806161	2207	139637
1879	13	2213	127750
1889	1276767	2237	111413
1901	647228	2243	125348
1907	604030	2251	1
1913	728650	2267	125961
1931	686494	2273	94427
1933	6	2297	86430
1949	745280	2309	167373
1951	6	2333	69767
1973	589663	2339	105510
1979	654728	2351	77390
1987	4	2357	53390
1993	7	2381	55279
1997	421804	2393	63687
1999	8	2399	65831
2003	376504	2411	41961
2011	2	2417	43465
2017	3	2423	35076
2027	352557	2441	40153
2029	5	2447	32700
2039	492203	2459	44961
2053	1	2477	32421
2063	282915	2531	25026
2069	391980	2543	24048
2081	243703	2549	31649
2083	1	2579	29803
2087	228323	2591	17387
2089	3	2609	25507
2099	372320	2621	16527
2111	195307	2633	13667

Occurences of primes as q values for prime Q values (6)

prime	occurences of q	prime	occurences of q
2657	12736	3251	682
2663	12484	3257	633
2687	14142	3299	1009
2693	11514	3323	584
2699	15200	3329	794
2711	9690	3347	435
2729	17464	3359	844
2741	7402	3371	389
2753	7739	3389	493
2777	6598	3407	350
2789	9310	3413	326
2801	5563	3449	506
2819	7920	3461	258
2837	5781	3467	284
2843	4429	3491	261
2861	4523	3527	247
2879	5940	3533	239
2897	4754	3539	310
2903	3711	3557	180
2909	4780	3581	175
2927	2701	3593	179
2939	5096	3617	141
2957	2498	3623	143
2963	2687	3659	192
2969	3386	3671	104
2999	2847	3677	98
3011	1711	3701	106
3023	2002	3719	158
3041	1670	3761	103
3083	1290	3767	73
3089	2071	3779	148
3119	1942	3797	44
3137	1025	3803	62
3167	1012	3821	78
3191	1329	3833	64
3203	871	3851	52
3209	1100	3863	82
3221	793	3881	42

Occurences of primes as q values for prime Q values (7)

prime	occurences of q	prime	occurences of q
3911	37	4397	4
3917	41	4409	10
3923	51	4421	6
3929	48	4451	6
3947	36	4457	2
3989	78	4463	1
4001	32	4481	2
4007	25	4493	3
4013	29	4517	1
4019	43	4523	2
4049	26	4547	4
4073	28	4583	5
4079	20	4643	3
4091	16	4649	3
4127	17	4673	2
4133	13	4679	2
4139	16	4691	2
4157	12	4703	2
4211	15	4721	1
4217	12	4787	1
4229	12	4793	2
4241	10	4799	1
4253	8	4889	2
4259	13	4919	1
4271	5	4937	1
4283	3	4967	1
4289	11	5039	1
4337	3	5081	1
4349	6	5189	1
4373	9	5237	1
4391	3	5477	1

Records of prime Q values (1)

value of Q	ordinal number of q among primes	value of q
2	1	2
3	2	3
7	3	5
13	4	7
31	6	13
89	7	17
101	9	23
311	20	71
1439	24	89
2213	41	179
6089	52	239
11777	54	251
32003	71	353
145043	72	359
266159	77	389
380729	81	419
381419	89	461
386237	116	641
569603	119	653
7988117	135	761
9108629	165	977
19888217	166	983
24911213	186	1109
32041007	200	1223
101281217	227	1433
235108859	228	1439
238192517	267	1709
1135483247	280	1811
2057684873	292	1907
3323353493	342	2297
3453752117	386	2663
15815934257	416	2861
55276074839	417	2879
80843887847	424	2939
129227135969	428	2969
170541844169	454	3209
221878587977	463	3299
486163786223	511	3659

Records of prime Q values (2)

value of Q	ordinal number of q among primes	value of q
622058767703	545	3929
1656084897563	577	4217
3586302052007	594	4349
5902078624073	616	4547
11395592256779	654	4889
29177415849833	664	4967
37374762984887	679	5081
41412971528939	723	5477

Occurences of primes as q values for composite Q values (1)

prime	occurences of q	prime	occurences of q
2	1	97	279958845
3	4697664044	101	634188808
5	6394420025	103	185185398
7	3853168770	107	547152657
11	5194491566	109	219021062
13	3439663112	113	451502282
17	4074615749	127	114183497
19	2780127375	131	406492386
23	3290730487	137	369511610
29	3648964834	139	128657362
31	1471903767	149	382787463
37	1348653795	151	66196047
41	2496359898	157	52104770
43	1062986565	163	49297857
47	1738469301	167	276030470
53	1540528412	173	199483368
59	1732700772	179	243308313
61	605450504	181	41523761
67	551719187	191	160501874
71	1058128005	193	22360443
73	402358330	197	156437724
79	482905082	199	27074814
83	951749579	211	18106835
89	930105049	223	17440439

Occurences of primes as q values for composite Q values (2)

prime	occurences of q	prime	occurences of q
227	118094700	449	14591239
229	17302362	457	184296
233	107954371	461	11393182
239	120880873	463	140579
241	9300093	467	8943631
251	94941752	479	9503194
257	68655217	487	104572
263	68474836	491	6114470
269	74209134	499	128669
271	4783233	503	6684509
277	4259950	509	7300473
281	49680471	521	4114632
283	3414761	523	46295
293	49855419	541	55862
307	3881816	547	50404
311	39065812	557	4403667
313	2083316	563	3525633
317	36023486	569	4801907
331	2133571	571	43815
337	1835585	577	28080
347	30864688	587	3625820
349	2382774	593	2657101
353	26186149	599	3292562
359	33552618	601	25740
367	920503	607	16456
373	1030442	613	14700
379	1255080	617	2243562
383	20023429	619	18932
389	28849183	631	13545
397	529880	641	1800443
401	16860820	643	11933
409	631245	647	1689787
419	23782097	653	1466751
421	395294	659	2201117
431	12551893	661	6373
433	348171	673	5663
439	396632	677	1249383
443	10769508	683	1101220

Occurences of primes as q values for composite Q values (3)

prime	occurences of q	prime	occurences of q
691	5041	967	89
701	1072151	971	130378
709	5712	977	137624
719	1264450	983	129626
727	3934	991	96
733	2283	997	47
739	3768	1009	99
743	755626	1013	112578
751	2180	1019	158169
757	1864	1021	73
761	750725	1031	93117
769	2863	1033	47
773	589348	1039	40
787	1080	1049	138828
797	822511	1051	27
809	766807	1061	66527
811	1172	1063	30
821	502981	1069	18
823	709	1087	23
827	490929	1091	79237
829	799	1093	15
839	671773	1097	59807
853	518	1103	54775
857	410918	1109	72590
859	547	1117	11
863	292053	1123	7
877	305	1129	10
881	361019	1151	36579
883	266	1153	5
887	251428	1163	41058
907	189	1171	8
911	244407	1181	30219
919	276	1187	39731
929	290321	1193	30037
937	130	1201	1
941	182024	1213	4
947	185512	1217	38046
953	163273	1223	25449

Occurences of primes as q values for composite Q values (4)

prime	occurences of q	prime	occurences of q
1229	33073	1637	1695
1231	4	1667	1189
1237	1	1697	775
1249	3	1709	1364
1259	35049	1721	964
1277	18218	1733	688
1279	2	1787	645
1283	16235	1811	501
1289	23282	1823	492
1291	1	1847	678
1301	15760	1871	462
1307	11921	1877	418
1319	16305	1889	583
1321	3	1901	308
1361	8258	1907	295
1367	10274	1913	326
1373	8471	1931	314
1381	1	1949	319
1409	11592	1973	237
1427	8363	1979	262
1429	1	1997	175
1433	5178	2003	157
1439	7795	2027	131
1451	5437	2039	188
1481	4313	2063	99
1487	4000	2069	140
1493	3716	2081	96
1499	4881	2087	100
1511	3369	2099	133
1523	2608	2111	95
1553	3133	2129	98
1559	3375	2141	71
1571	1705	2153	56
1583	2004	2207	50
1601	1500	2213	38
1607	1743	2237	30
1613	1229	2243	41
1619	2032	2267	39

Occurences of primes as q values for composite Q values (5)

prime	occurences of q	prime	occurences of q
2273	21	2591	4
2297	24	2609	3
2309	46	2621	3
2333	18	2633	3
2339	30	2657	3
2351	10	2663	3
2357	16	2687	6
2381	11	2693	1
2393	15	2699	2
2399	15	2711	1
2411	10	2741	1
2417	9	2753	1
2423	8	2789	1
2441	10	2861	2
2447	6	2879	3
2459	4	2897	2
2477	8	2909	1
2531	11	2939	2
2543	8	2957	1
2549	7	2963	1
2579	9	3329	1

Records of composite Q values (1)

value of Q	ordinal number of q among primes	value of q
2	1	2
3	2	3
7	3	5
13	4	7
31	6	13
51	8	19
101	9	23
219	10	29
309	11	31
311	20	71
1439	24	89

Records of composite Q values (2)

value of Q	ordinal number of q among primes	value of q
2213	41	179
6089	52	239
11333	69	347
32003	71	353
83633	86	443
260699	89	461
345113	96	503
386237	116	641
569603	119	653
250004003	123	677
250225553	148	857
250370591	161	947
251532719	178	1061
252008903	186	1109
252779399	212	1301
261799079	223	1409
263491517	245	1553
482483669	290	1889
1447688453	304	2003
2767849277	317	2099
3323353493	342	2297
3453752117	386	2663
9205237187	427	2963
94129907513	469	3329

References

[1] **Kátai I.,** On sets characterizing number theoretical functions, *Acta Arith.*, **13** (1968), 315-320.

[2] **Kátai I.,** On sets characterizing number theoretical functions II., *Acta Arith.*, **16** (1968), 1-4.

[3] **Elliot P.D.T.A.,** A conjecture of Kátai, *Acta Arith.*, **26** (1974), 11-20.

[4] **Wolke D.,** Bemerkungen über Eindeutigkeitsmengen additiver Funktionen, *Elem. der Math.*, **33** (1978), 14-16.

[5] **Dress F. et Volkman B.,** Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives, *C.R. Acad. Sci. Paris, Sér. A-B,* **287** (1978), 43-46.

[6] **Meyer J.,** Ensembles d'unicité pour les fonctions additives. Étude analogue dans le cas des fonctions multiplicatives, Conf. on Analytic and Elementary Number Theory, Orsay, 1980, *Publ. Math. Orsay,* **81** (1), Univ. Paris XI, Orsay, 1981, 50-66.

[7] **Indlekofer K.-H.,** On sets characterizing additive and multiplicative arithmetical functions, *Illinois J. Math.,* **25** (1981), 251-257.

[8] **Schinkel A. and Sierpinski W.,** Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.,* **8** (1958), 185-208.

[9] **Elliot P.D.T.A.,** On representing integers as products of the $p+1$, *Monatshefte für Math.,* **97** (1984), 85-97.

[10] **Ribenboim P.,** *The new book of prime number records,* Springer Verlag, New York, 1995.

[11] **Caldwell C.,** *Finding primes and proving primality,* Chapter Two. Strong probable-primality and a practical test
`http://primes.utm.edu/prove/prove2_3.html`

[12] **Pomerance C., Selfridge J.L. and Wagstaff S.S.Jr.,** The pseudoprimes to $25 \cdot 10^9$, *Math. Comp.,* **35** (1980), 1003-1026.

[13] **Jaeschke G.,** On strong pseudoprimes to several bases, *Math. Comp.,* **61** (1993), 915-926.

[14] **Sloane N.J.A.,** *On-line encyclopedia of integer sequences*
`http://www.research.att.com/~njas/sequences/`

[15] **AMD Developer Center,** *Documentations*
`http://developer.amd.com/documentation.jsp`

[16] *Condor Project Homepage* `http://www.cs.wisc.edu/condor/`

T. Csajbók, A. Járai and J. Kasza
Department of Computer Algebra
Eötvös Loránd University
Pázmány Péter sét. 1/C
H-1117 Budapest, Hungary